IN THE CLAIMS:

Please amend claim 1 as follows:

1. (currently amended) A method for purchasing items over a network using a secure communication device, the secure communication device including a host processor, a secure memory that includes a laser-scribed encryption key, and a non-secure memory for storing encrypted data, wherein sensitive data is encrypted within the secure memory using the laser-scribed encryption key and stored as encrypted data in the non-secure memory, the method comprising the steps of:

retrieving an encrypted credit card number and an encrypted secret key from the non-secure memory;

decrypting the encrypted credit card and secret key with the laser-scribed encryption key; encrypting the credit card number with a communication encryption key, the communication encryption key being related to the secret key; and

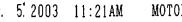
and transferring the credit card number, as encrypted with the communication encryption key, over the network to a destination.

- 2. (original) The method as claimed in claim 1 wherein the encrypted data is decrypted within the secure memory using the laser-scribed encryption key and stored within the secure memory for use by the host processor.
- 3. (original) The method as claimed in claim 1 further comprising the steps of: receiving a personal identification number (PIN) from a user; decrypting an encrypted PIN with the laser-scribed encryption key; wherein the step of transferring the encrypted credit card number step is performed when the decrypted PIN and the PIN received from the user compare.
 - 4. (original) The method as claimed in claim 1 further comprising the steps of: receiving biometric information from a user; decrypting stored biometric information for the user with the laser-scribed encryption

wherein the step of transferring the encrypted credit card number step is performed when the decrypted biometric information compares with the biometric information received from the user.



key;



- 5. (original) The method as claimed in claim I wherein the communication encryption key is a common session key and wherein the method further comprises the step of generating the session key using the secret key and information provided by the destination.
- 6. (original) The method as claimed in claim 1 wherein the host processor and secure memory are fabricated on an integrated circuit chip, and the encrypted data is stored in a nonvolatile memory.
- 7. (original) The method as claimed in claim 1 wherein the laser-scribed encryption key is generated by laser-scribing a semiconductor die during fabrication of the secure memory to create a plurality of fixed "ones" and "zeroes" which make up the laser-scribed encryption key.
- 8. (original) The method as claimed in claim 1 wherein the laser-scribed encryption key is generated burning one-time programmable fuses on a semiconductor die during fabrication of the secure memory to create a plurality of fixed "ones" and "zeroes" which make up the laser-scribed encryption key.
- 9. (original) The method as claimed in claim 1 wherein the secure memory includes blocking gates coupled between the laser-scribed encryption key and encryption logic circuitry, the blocking gates being comprised of logic gates and have a blocking control signal input preventing access to the laser-scribed encryption key by the encryption logic circuitry.
- 10. (original) The method as claimed in claim 1 wherein the laser-scribed encryption key is unique for each secure memory of a plurality of secure memories of different processing systems.
- (original) The method as claimed in claim 1 wherein the laser-scribed encryption key is randomly generated for each secure memory of a plurality of secure memories of different processing systems.
- 12. (original) A method for transferring sensitive data over a non-secure communication channel using a secure communication device, the secure communication device including a host processor, a secure memory that including a laser-scribed encryption key, and a non-secure memory for storing the sensitive data in encrypted form, wherein sensitive data is encrypted within the secure memory using the laser-scribed encryption key and stored as encrypted data in



the non-secure memory, the method comprising the steps of:

retrieving the encrypted sensitive data and an encrypted secret key from the non-secure memory;

decrypting, in the secure memory, the encrypted sensitive data and the secret key with the laser-scribed encryption key;

encrypting the decrypted sensitive data with a session encryption key related to the secret key; and

transferring the sensitive data encrypted with the session encryption key over the non-secure communication channel to a destination.

13. (original) The method as claimed in claim 12 further comprising the steps of: receiving biometric information from a user;

decrypting stored biometric information for the user with the laser-scribed encryption key;

wherein the step of transferring the encrypted sensitive data step is performed when the decrypted biometric information compares with the biometric information received from the user.

- 14. (original) The method as claimed in claim 12 wherein the host processor and secure memory are fabricated on an integrated circuit chip, and the encrypted data is stored in a non-volatile memory.
- 15. (original) The method as claimed in claim 12 wherein the laser-scribed encryption key is generated by laser-scribing a semiconductor die during fabrication of the secure memory to create a plurality of fixed "ones" and "zeroes" which make up the laser-scribed encryption key.
- 16. (original) The method as claimed in claim 12 wherein the laser-scribed encryption key is generated by burning one-time programmable fuses on a semiconductor die during fabrication of the secure memory to create a plurality of fixed "ones" and "zeroes" which make up the laser-scribed encryption key.
- 17. (original) The method as claimed in claim 12 wherein the secure memory includes blocking gates coupled between the laser-scribed encryption key and encryption logic circuitry, the blocking gates being comprised of logic gates and have a blocking control signal input preventing access to the laser-scribed encryption key by the encryption logic circuitry.





- 18. (original) The method as claimed in claim 12 wherein the laser-scribed encryption key is randomly generated for each secure memory of a plurality of secure memories of different processing systems.
- 19. (original) The method as claimed in claim 12 wherein the laser-scribed encryption key is unique for each secure memory of a plurality of secure memorics of different processing systems.